REMARKS

The present application was filed on December 28, 1999 with claims 1-15. New claims 16-25 were subsequently added by amendment. Claims 1-25 are currently pending, with claims 1, 6-10 and 22 being the independent claims.

Claims 1-25 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,167,469 (hereinafter "Safai") in view of U.S. Patent No. 6,788,336 (hereinafter "Silverbrook"), U.S. Patent No. 5,732,138 (hereinafter "Noll"), and RFC1750 by Eastlake et al. entitled "Randomness Recommendations for Security" (hereinafter "Eastlake").

In this response, Applicants respectfully traverse the §103(a) rejection.

Independent claim 1 recites a digital camera having a processor that generates a random seed entirely from sensor noise within the digital camera. The processor is further specified as using the random seed to generate a private key and a public key. The private key is stored in a memory in the digital camera for subsequent use in encryption of a hash of a digital image to produce an image authentication signature. This approach advantageously overcomes a number of problems associated with conventional arrangements. For example, it avoids the serious security concerns that can arise when a manufacturer or user has to generate a private key external to the camera and subsequently load the private key into the camera. See the specification at page 1, line 20, to page 2, line 16, and page 2, lines 25-30.

Applicants initially note that a proper *prima facie* case of obviousness under §103(a) requires that the cited references must teach or suggest all the claim limitations, and that there be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify or combine the reference teachings. See Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(j).

Applicants submit that the Examiner has failed to establish a proper *prima facie* case of obviousness in the §103(a) rejection of claims 1-25, in that the proposed combination of references fails to teach or suggest all the limitations of the claims, and in that no cogent motivation has been identified for modifying or combining the reference teachings to reach the claimed invention.

With regard to independent claim 1, the Examiner in formulating the §103(a) rejection argues that the combined teachings of Safai, Silverbrook, Noll and Eastlake meet each and every limitation of the claim. The Examiner characterizes Safai as teaching "a processor located within the digital camera for generating [a] private key and a public key," relying on column 4, lines 1-15, column 7, lines 30-40, and claim 29 of Safai. See the final Office Action at page 4, section 4. Applicants respectfully disagree with this characterization of Safai. There is no teaching or suggestion in Safai to the effect that a private key is generated within a digital camera. At column 16, lines 29-30, Safai indicates that a private key is "stored in the camera," but <u>nowhere does Safai disclose that the private key that is stored in the camera is generated within the camera itself</u>. The portions of the Safai reference relied on by the Examiner in this regard fail to indicate with specificity that the private key is generated within the camera, and to the contrary are entirely consistent with generation of the private key external to the camera as in the conventional arrangements described by Applicants at page 1, line 20, to page 2, line 16, of their specification.

In the final Office Action at page 2, section 2, first paragraph, the Examiner further argues that the teachings in Safai at column 4, lines 9-12, and claim 29, indicate that the generation of the private key in Safai is performed within the digital camera. However, Applicants note that a number of the claims which depend from independent claim 1 in Safai clearly recite operations that do not occur in a digital camera, despite the general recitation in their parent claim. See, for example, claim 23, which states that the transporting step of claim 1 further includes the steps of printing a tangible copy of an image and sending the tangible copy of the image to an addressee. Clearly, these steps do not occur in the digital camera, although the parent claim 1 states that the general method is "in a digital camera." Another example is dependent claim 24, which indicates that the sending step of claim 23, which is part of the transporting step of claim 1, includes sending the tangible copy to the addressee using a common carrier. Again, such a step clearly does not occur in a digital camera. The point of this argument is that the Examiner cannot reasonably conclude that <u>every step</u> recited in every claim dependent from claim 1 in Safai <u>necessarily occurs in a digital</u>

camera. Thus, Applicants submit that there is no teaching in the relied-upon portions of Safai to the effect that the private key disclosed therein is generated in a digital camera.

Furthermore, there is additional evidence in Safai itself that the private key disclosed therein is not generated by a processor of the digital camera 100. For example, Safai at column 16, lines 31-32, indicates that the private key is stored in the digital camera in a manner that prevents recovery. More specifically, the private key is "embedded in firmware within the camera." At column 1, lines 27-31, Safai indicates that such firmware is typically read-only memory (ROM). These teachings would tend to indicate that the private key is generated outside the digital camera and stored in firmware thereof at the time of manufacture. Such an approach is entirely conventional, and particularly problematic, as described by Applicants in the background portion of their specification at page 1, line 20, to page 2, line 4.

Moreover, Applicants note that the recited digital camera processor of claim 1 of the present application uses the random seed to generate a private key and a public key. As indicated above, the Examiner argues that Safai teaches such a processor located within a digital camera. However, the relied-upon portions of Safai do not make any mention whatsoever of generation of a public key using a processor of a digital camera, and to the contrary appear to teach away from such an arrangement. See Safai at, for example, column 16, lines 26-29, which simply indicates that a public key for the digital camera 100 is stored at server 601. There is clearly no processor in the digital camera 100 of Safai that generates both a private key and a public key.

Thus, it appears that the Examiner has mischaracterized the teachings of Safai in formulating the §103(a) rejection, and that Safai would suffer from the very same problems as the conventional arrangements identified by Applicants in their specification.

The Examiner acknowledges certain deficiencies in Safai as applied to claim 1, but argues that these deficiencies are overcome by teachings in Silverbrook, Noll and Eastlake. See the final Office Action at pages 4-6. Applicants respectfully disagree. The collective teachings of Safai, Silverbrook, Noll and Eastlake do not teach or suggest a digital camera having a processor that generates a random seed entirely from sensor noise within the digital camera and then uses the random seed to generate a private key and a public key. Silverbrook at column 204, lines 9-19, references the lava lamp based system of Noll as a potential source of random numbers. Thus, Silverbrook is looking to random sources that are external to the digital camera unit 1 of FIG. 1 in Silverbrook. The lava lamp based system of Noll uses a separate digital camera to photograph lava lamps, and then processes the resulting images to obtain a seed. See Noll at column 4, line 46, to column 5, line 19, and column 6, lines 24-27. It is therefore apparent that Silverbrook is suggesting that a source external to the digital camera unit 1 of FIG. 1 in Silverbrook should be used as a source of random numbers. This is directly contrary to the claimed arrangement in which a digital camera includes a processor that generates a random seed entirely from sensor noise within the digital camera and then uses the random seed to generate a private key and a public key. Accordingly, it is believed that the relied-upon portions of Silverbrook and Noll actually teach away from the claimed invention.

The Examiner at page 2, last paragraph, to page 3, first paragraph, of the final Office Action further argues that Noll is not limited to lava lamps, but more generally applies to any "chaotic system," citing column 4, lines 43-45, column 6, line 66, to column 7, line 11, and claims 1, 8 and 14 of Noll. However, Applicants are not arguing that Noll is limited to digitized images of lava lamps. What Applicants are arguing is that Silverbrook relies on sources external to a digital camera, and any such source taken from Noll would still be arranged external to the digital camera in Silverbrook. Noll in its general statements and claims teaches that a state of a chaotic system is digitized, but Silverbrook nonetheless teaches to treat any such source from Noll as source of randomness that is external to the digital camera unit 1 of FIG. 1.

The Eastlake reference fails to supplement the above-described deficiencies of Silverbrook, Noll and Safai as applied to claim 1. The relied-upon portion of Eastlake, at section 5.3.1, describes an arrangement in which a computer system uses an external video input supplied from a camera as a source of random bits. Such an arrangement is similar to what is described in Noll, where the output of an image-based system is used as an external source of randomness for another system. See step 600 in the flow diagram in FIG. 6 of Noll, where a seed obtained by processing the images of the lava lamps is used as an external source input to a pseudo-random number generator. See Noll at column 6, lines 21-35. There is no suggestion in Eastlake that the camera use its own sensor noise to generate its own random seed. To the contrary, Eastlake teaches that the camera output is used as an external source input to a separate computer system.

Accordingly, it is believed that the combined teachings of Safai, Silverbrook, Noll and Eastlake fail to meet the limitations of independent claim 1.

Furthermore, it is believed that insufficient objective evidence of motivation to combine Safai, Silverbrook, Noll and Eastlake has been identified by the Examiner.

The Federal Circuit has stated that when patentability turns on the question of obviousness, the obviousness determination "must be based on objective evidence of record" and that "this precedent has been reinforced in myriad decisions, and cannot be dispensed with." In re Sang-Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). Moreover, the Federal Circuit has stated that "conclusory statements" by an examiner fail to adequately address the factual question of motivation, which is material to patentability and cannot be resolved "on subjective belief and unknown authority." Id. at 1343-1344.

The Examiner identifies alleged motivation for the proposed combination of Safai, Silverbrook, Noll and Eastlake at pages 5-6 of the final Office Action. Applicants respectfully submit that the proffered statements of motivation are conclusory in nature or otherwise insufficient. For example, the Examiner at page 5, lines 5-6, indicates that one motivation for the combination would be "to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing." Applicants believe that this alleged motivation goes primarily to the strength of the private and public keys, and not to where they are generated, and therefore fails to address the limitations at issue in the claim. Safai alone, for instance, could increase the strength of its keys against compromise by guessing, by simply using longer key lengths or other similar conventional arrangements. Accordingly, this proffered statement of motivation fails to support the particular combination in question. Points [1] and [2] of page 6, first paragraph, of the final Office Action also appear to relate to strength of the generated keys, and not to where the keys are generated, and thus fail to address the limitations at issue. Furthermore, the Examiner in point [3] on page 6, first paragraph, argues that the proposed combination is motivated because it would "obviate the need . . . to carry additional cumbersome hardware." This is conclusory because it relies on an advantage of the claimed invention as alleged motivation for combination of the references. None of the references themselves provide any objective evidence to support this alleged motivation. As noted above, Silverbrook clearly teaches to use an external random source, such as the lava lamp based system of Noll or some other external source as in Eastlake, which is a direct teaching away from the present invention.

It therefore appears that the Examiner in formulating the §103(a) rejection of claim 1 over Safai, Silverbrook, Noll and Eastlake has undertaken a piecemeal reconstruction of the claimed invention based upon impermissible hindsight, given the benefit of the disclosure provided by Applicants.

Independent claims 6-10 and 22 are believed allowable for reasons similar to those identified above with regard to claim 1.

Applicants had previously amended independent claims 6, 7, 8 and 10 to clarify that the generation of the private key, or private key and public key, occurs in the digital camera.

For example, independent claims 7, 8, 9, 10 each recite generation of both a private key and a public key in a digital camera.

In characterizing the Safai reference in the context of formulating the §103(a) rejection of these independent claims, the Examiner argues that Safai teaches the generation of both a private key and a public key within a digital camera. See, for example, page 6, bottom of the page, step (a), of the final Office Action. This is believed to be a clear mischaracterization of Safai. As Applicants described above in the context of claim 1, Safai fails to teach or suggest the generation of a private key within a digital camera, much less the generation of both a private key and a public key within a digital camera. Although Safai makes reference to private and public keys, their generation in Safai is believed to suffer from the very problems identified by Applicants at page 1, line 20, to page 2, line 4, in the background portion of the present specification. The Silverbrook, Noll and Eastlake references fail to supplement the fundamental deficiencies of Safai as applied to the independent claims, in that such references at best collectively teach to utilize an external source of randomness as an input to another system.

The dependent claims are believed allowable at least by virtue of their dependence from their respective independent claims, and are also believed to define additional patentable subject matter over the proposed combination of Safai, Silverbrook, Noll and Eastlake.

In view of the foregoing it is respectfully submitted that the claims in their present form are in condition for allowance and such action is respectfully requested.

As indicated previously, a Notice of Appeal is submitted concurrently herewith.

The Commissioner is hereby authorized to charge any fees in connection with this communication to Deposit Account No. 05-0225.

Respectfully submitted,

Attorney for Applicant(s)
Registration No. 53,950

Thomas J. Strouse/phw
Rochester, NY 14650
Telephone: 585-588-2728
Facsimile: 585-477-4646

If the Examiner is unable to reach the Applicant(s) Attorney at the telephone number provided, the Examiner is requested to communicate with Eastman Kodak Company Patent Operations at (585) 477-4656.